APLIKASI PENGIRIMAN PESAN PENGKODEAN MENGGUNAKAN METODE AES 128 BIT BERBASIS ANDROID

SKRIPSI

Diajukanoleh :

YUDITH ADI SUCAHYO
NPM : 0734010025

Kepada

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"

JAWA TIMUR

2012

KATA PENGANTAR

Dengan mengucapkan puji syukur kehadirat Alloh SWT atas rahmat serta hidayahnya yang diberikan sehingga dapa tmenyelesaikan Tugas Akhir ini dengan baik dan tepat waktu dimana hasilnya disusun dengan bentuk laporan yang berjudul Aplikasi Pengiriman Pesan Pengkodean Menggunakan Metode AES 128 bit berbasis Android.

Adapun laporan ini disusun yaitu untuk memenuhi syarat mengikuti seminar TA serta untuk memenuhi syarat kelulusan salah satu mata kuliah "TugasAkhir" di Universitas Pembangunan Nasioanal "Veteran" JawaTimur.

Penulis menyadari bahwa manusia yang serba kurang sempurna, maka di dalam upaya menyusun Tugas Akhir ini peneliti telah banyak memperoleh bantuan dan bimbingan dari berbagai pihak, mengingat keterbatasan pengalaman yang dimiliki oleh peneliti, sehingga penulis sangat mengharapkan segala kritik dan saran yang konstruktif dan membangun demi kebaikan maupun sistematika penulisan akan selalu peneliti terima dengan senang hati guna kesempurnaan Tugas Akhir ini. Harapan peneliti mudah – mudahan apa yang penulis lakukan ini dapat menjadi sumbangan pemikiran dan berguna bagi semuanya, terutamaUniversitas Pembangunan Nasional "Veteran" JawaTimur.

Surabaya, Desember 2012

Yudith Adi Sucahyo

UCAPAN TERIMA KASIH

Dalam pembuat laporan ini, peneliti telah mendapatkan bantuan dan bimbingan dari berbagai pihak yang terkait, baik secara moril maupun materiil oleh karena itu pada kesempatan kali ini peneliti ingin menyampaikan ucapan terima kasih kepada:

1. Bapak Prof. Dr. IrTeguhSoedarto, MP. Selaku Rektor Universitas Pembangunan Nasional “Veteran” JawaTimur Surabaya.
2. Bapak Ir. Sutiyono, MT selaku Dekan Fakultas Teknologi Industri.
3. Ibu Dr.Ir. Ni Ketut Sari, MT,selaku Kepala Jurusan Teknik Informatika Universitas Pembangunan Nasional ”Veteran” Jawa Timur.
4. Bapak Hudan Studiawan, S.Kom, M.kom, sebagai Dosen Pembimbing yang telah meluangkan waktu dan memberikan bimbingan serta petunjuk selama menyusun Tugas Akhir ini.
5. Para Dosen Penguji Seminar : Barry Nuqoba, S.Si, M.Kom, Ir.Mu’tasim Billah, MS yang telah membuka wawasan baru bagi peneliti.
6. Para Dosen Penguji Lisan : Ir.Mu’tasim Billah, MS, Harianto, S.Kom, M.eng, Achmad Junaidi, S.Kom yang telah memberikan masukan positif kepada peneliti.
7. Kedua Orang Tua tercinta serta keluarga yang telah memberikan doa dan semangat kepada penulis.
8. Teman-teman peneliti : Untuk teman-teman seangkatan Oshin, Juzz’Sari, Vera, Trea, Faisol, Nanang, Rizal, Tobib, Gigih, Ardi, Novan dan teman seangkatan

lainya. yang tidak mungkin ditulis satu per satu terima kasih atas dukungan dan kebersamaanya selama empat tahun terakhir.

9. Kepada teman-teman KKN 41 love you all dan kepada Dody asmara,Edwin prasetyo terima kasih yang telah mensupport agar cepat selesai Tugas Akhir ini.

Surabaya, Januari 2013

Yudith Adi Sucahyo

DAFTAR ISI

APLIKASI PENGIRIMAN PESAN PENGKODEAN MENGGUNAKAN METODE AES 128 BIT BERBASIS ANDROID

Disusun Oleh : Yudith Adi Sucahyo

Dosen Pembimbing I : Hudan Studiawan S.kom, M.Kom

Abstraksi

Operating system Android merupakan operating system yang banyak digunakan pada smartphone maupun tablet pc. Perkembangan android secara pesat dikarenakan berbasis open source sehingga memudahkan developer untuk menciptakan aplikasi-aplikasi pendukung yang memberi manfaat bagi pengguna. Smart phone atau pun tablet pc mempunyai banyak fungsi. Aplikasi yang pasti digunakan oleh setiap orang adalah aplikasi pengiriman pesan pendek atau Short Message Standart (SMS).Pengiriman pesan pendek menjadi pilihan utama dalam berkomunikasi oleh pengguna.

Teknologi pengiriman pesan pendek saat ini menggunakan algoritma 64 bit untuk melakukan pengkodean. Berdasar permasalahan ini dalam melakukan penelitian dan pembuatan aplikasi pesan pendek yang menggunakan pengkodean pada AES 128 bit. Aplikasi ini dapat menjamin kerahasiaan isi pesan dengan melakukan perubahan pengkodean. Adanya fitur password menambah kekuatan dari aplikasi ini sehingga tidak bisa dibuka oleh user lain.

Pada percobaan yang dilakukan, aplikasi dapat berjalan dengan baik sesuai perancangan, yaitu dapat melakukan proses pengkodean AES 128 bit dan dekripsi untuk kembali membaca pesan yang telah di enkripsi. Aplikasi dapat berjalan di operating system android dengan lancar.

Kata Kunci : Android, Pengkodean, AES 128 bit

BAB I

PENDAHULUAN

1.1. Latar Belakang

Teknologi komunikasi kian berkembang pesat, belum lama mengenal gadget berbasis Java, Symbian, Lalu Blackberry, kini dengan disuguhkan teknologi Operating System yang diberi nama Android. Android adalah sistem operasi berbasis Linux yang saat ini banyak di gunakan untuk smart phone dan tablet computer. Android memberi kemudahan dengan menyediakan platform terbuka (open source) bagi para pengembang aplikasi untuk menciptakan aplikasi sendiri. Salah satu aplikasi berbasis android adalah aplikasi pengiriman pesan pendek.

Adanya kemungkinan penyadapan data, maka aspek keamanan dalam pertukaran informasi menjadi sangat penting karena suatu komunikasi data jarak jauh belum tentu memiliki jalur transmisi yang aman dari penyadapan sehingga keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri. Terdapat data-data yang tidak terlalu penting, sehingga apabila publik mengetahui data tersebut, pemilik data tidak terlalu dirugikan. Tetapi apabila pemilik data adalah pihak militer atau pemerintah, keamanan dalam pertukaran informasi menjadi sangat penting karena data yang dikirim kebanyakan adalah data-data rahasia yang tidak boleh diketahui oleh publik.

Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. Kriptografi merupakan kajian ilmu dan seni untuk menjaga suatu pesan atau data informasi agar data tersebut aman.

Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu secrecy (perlindungan terhadap kerahasiaan data informasi) dan authenticity (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan). Algoritma kriptografi yang baik akan memerlukan waktu yang lama untuk memecahkan data yang telah disandikan. Seiring dengan perkembangan teknologi komputer maka dunia teknologi informasi membutuhkan algoritma kripografi yang lebih kuat dan aman. Saat ini, AES (Advanced Encryption Standard) digunakan sebagai standar algoritma kriptografi yang terbaru. AES menggantikan DES (Data Encryption Standar) yang pada tahun 2002 sudah berakhir masa penggunaannya. DES juga dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat. AES sendiri adalah algoritma kriptografi dengan menggunakan algoritma Rijndael yang dapat mengenkripsi dan mendekripsiblok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit.

Berdasarkan permasalahan tersebut, pada penelitian tugas akhir kali ini, peneliti akan membuat aplikasi pengiriman pesan dengan menggunakan algoritma AES dengan panjang kunci 128 bit untuk handset berbasis Android. Sehingga isi pesan melalu media pengiriman pesan pendek tidak dengan mudah diketahui oleh orang lain.

1.2. Perumusan Masalah

Rumusan masalah yang digunakan dalam tugas akhir ini adalah :

1. Bagaimana membuat proses encode menggunakan algoritma AES dengan panjang kunci 128 bit pada handset berbasis android ?
2. Bagaimana membuat proses decode menggunakan algoritma AES dengan panjang kunci 128 bit pada handset berbasis android ?

1.3. Batasan Masalah

Pada tugas akhir ini batasan masalah yang dipergunakan yaitu :

1. Algoritma yang digunakan adalah AES dengan panjang kunci 128 bit.
2. Penelitian ini tidak membahas waktu komputasi yang dibutuhkan saat melakukan pengkodean dan juga waktu pengiriman pesan serta keberhasilan proses pengiriman pesan.
3. Software developer menggunakan Eclipse Helios.
4. Sistem operasi yang dipergunakan adalah Android minimal ver 2.2 (Froyo).

1.4. Tujuan

Tujuan yang ingin dicapai pada pengerjaan tugas akhir ini adalah: Membangun aplikasi yang dapat mengirimkan pesan algoritma AES dengan panjang kunci 128 bit untuk handset berbasis android.

1.5. Manfaat

Adapun manfaat yang ingin diperoleh dari pengerjaan tugas akhir ini adalah dapat membuat perangkat lunak untuk mempermudah pengguna handset

android dalam mengamankan pengiriman pesan dengan menggunakan algoritma AES dengan panjang kunci 128 bit.

1.6. Sistematika Penulisan

Sistematika penulisan tugas akhir ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, identifikasi masalah, maksud dan tujuan yang ingin dicapai, batasan masalah, metodologi penelitian yang diterapkan dalam memperoleh dan mengumpulkan data, waktu dan tempat penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik masalah yang diambil dan hal-hal yang berguna dalam proses analisis permasalahan.

BAB III ANALISIS DAN PERANCANGAN

Membahas metode penelitian dan menganalisis masalah dari model penelitian untuk memperlihatkan keterkaitan antar variabel yang diteliti serta perancangan sistem yang akan dibuat.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Membahas mengenai pengimplementasian aplikasi yang telah dibuat ke perangkat yang akan digunakan serta melakukan pengujian terhadap aplikasi yang telah diimplementasikan tersebut.

BAB V PENUTUP

Berisi kesimpulan dan saran yang sudah diperoleh dari hasil penulisan tugas akhir.

BAB VI KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil analisis dan pengolahan data serta saran-saran yang dapat dijadikan bahan masukan untuk pengembangan sistem selanjutnya.